



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF COUNTY AUDIT
SUITE 1500
JAMES K. POLK STATE OFFICE BUILDING
NASHVILLE, TENNESSEE 37243-0269
PHONE (615) 401-7841

April 19, 2005

Marion County Mayor and
Board of County Commissioners
Marion County, Tennessee

To the County Mayor and County Commissioners:

In conjunction with the annual audit of Marion County, we have performed a limited review of the information systems in the Offices of County Mayor, Highway Superintendent, Director of Schools, Trustee, County Clerk, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, and Sheriff as of March 17, 2005. This letter transmits the results of our review.

Our audit of Marion County is required to be conducted in accordance with standards contained in Government Auditing Standards, issued by the Comptroller General of the United States. These standards specify that we perform general and application control reviews of computer-based accounting and information systems to determine whether an entity's existing procedures and controls provide adequate assurance of data accuracy and financial and operating statement reliability.

Because of inherent limitations in any internal control structure, errors, irregularities, or control weaknesses may exist and may not be detected. However, our information system reviews performed in the Offices of County Mayor, Highway Superintendent, Trustee, County Clerk, Clerk and Master, and Register did not reveal any matters that we considered to be a reportable condition. Reportable conditions were identified in the Offices of Director of Schools, Circuit and General Sessions Courts Clerk, and Sheriff. These reportable conditions may be included in the annual financial report of Marion County. These matters are also presented in detail in the enclosed Review of Internal Controls Regarding Information System Operations — Findings and Recommendations.

A brief summary of the reportable conditions by office is presented below:

DIRECTOR OF SCHOOLS

1. The office did not develop a disaster recovery plan.

Marion County Mayor and
Board of County Commissioners
April 19, 2005
Page 2

CIRCUIT AND GENERAL SESSIONS COURTS CLERK

1. The office had not entered into a formal hardware and software maintenance contract.
2. The office did not develop a disaster recovery plan.

SHERIFF

1. The office had deficiencies in computer system back-up procedures.
2. The office did not implement adequate controls to protect its information resources against unauthorized access, modification, destruction, or disclosure.

Please contact Penny Austin, our Information Systems Audit Manager, or me if you have any questions regarding our review of the information systems in the aforementioned offices of Marion County, Tennessee.

Sincerely,



Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable John Graham, Highway Superintendent
The Honorable Fred Taylor, Director of Schools
The Honorable David Kirk, Trustee
The Honorable Dwight Minter, County Clerk
The Honorable Evelyn Griffith, Circuit and General Sessions Courts Clerk
The Honorable Levoy Gudger, Clerk and Master
The Honorable Winfred Haggard, Register
The Honorable Ronnie Burnett, Sheriff
Mr. Carl Lowe, Mid-East Tennessee Audit Manager

MARION COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION SYSTEM
OPERATIONS — FINDINGS AND RECOMMENDATIONS
AS OF MARCH 17, 2005

The review of controls over the information systems in the Offices of Director of Schools, Circuit and General Sessions Courts Clerk, and Sheriff indicated a need for improvement. It should be noted that this was the first information system review performed in the Office of Sheriff. The following findings and recommendations have been made to aid the offices in the implementation of controls to better secure their computer systems and the information contained therein. We reviewed these matters with management to provide an opportunity for their response. Management offered oral responses to these items but did not submit written responses. We did not include the oral responses in this report.

OFFICE OF DIRECTOR OF SCHOOLS

THE OFFICE DID NOT DEVELOP A DISASTER RECOVERY PLAN

1. FINDING

The office did not develop a disaster recovery plan to assist in re-creating its data processing environment in the event of a disaster. Without a formal, written plan, critical computerized applications could be disrupted indefinitely until the system could be repaired or a back-up facility could be found and made operational.

RECOMMENDATION

Management should develop and regularly update a disaster recovery plan defining procedures for personnel to follow in the event of a major hardware or software failure, or temporary or permanent destruction of facilities. The plan should contain provisions for a contingency operations site, as well as the adequate backup of data files, system programs, user documentation, supplies, and computer hardware so that operations could continue as normally as possible. A copy of the plan should be kept in a secure area within the office, as well as at a secure, off-site location.

OFFICE OF CIRCUIT AND GENERAL SESSIONS COURTS CLERK

THE OFFICE HAD NOT ENTERED INTO A FORMAL HARDWARE AND
SOFTWARE MAINTENANCE CONTRACT

1. FINDING

The office made payments to a vendor for hardware and software maintenance on the computer system located in the office. However, a formal written contract between Marion County and the vendor did not exist.

RECOMMENDATION

The office should enter into a formal written agreement with the vendor for hardware and software maintenance services to be provided by that vendor on the computer system located in the office. In addition, the contract should outline customer payment schedules. All service contracts of this nature should be filed and recorded centrally so that they are available for reference. Contracts should be reviewed periodically to ensure that they continue to provide required services.

THE OFFICE DID NOT DEVELOP A DISASTER RECOVERY PLAN

2. FINDING

The office did not develop a disaster recovery plan to assist in re-creating its data processing environment in the event of a disaster. Without a formal, written plan, critical computerized applications could be disrupted indefinitely until the system could be repaired or a back-up facility could be found and made operational.

RECOMMENDATION

Management should develop and regularly update a disaster recovery plan defining procedures for personnel to follow in the event of a major hardware or software failure, or temporary or permanent destruction of facilities. The plan should contain provisions for a contingency operations site, as well as the adequate backup of data files, system programs, user documentation, supplies, and computer hardware so that operations could continue as normally as possible. A copy of the plan should be kept in a secure area within the office, as well as at a secure, off-site location.

OFFICE OF SHERIFF

RECOMMENDATIONS

1. SYSTEM BACK-UP PROCEDURES SHOULD BE IMPROVED

The following procedures regarding the system back-up process should be implemented:

1. Daily system back-up procedures should be implemented. A backup labeled for each day of the week should be maintained. These backups should be stored in a secure, fireproof location.
2. In addition to daily system backups, a weekly system backup should be performed, and two copies of this backup should be maintained. These backups should be rotated off site on a weekly basis.
3. A secure, fireproof location should be used to store weekly backups. Some possibilities for an off-site storage location would be another county office building with a fireproof vault or a safe deposit box at a local bank.
4. A current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

2. **THE OFFICE SHOULD IMPLEMENT ADEQUATE CONTROLS TO PROTECT ITS INFORMATION RESOURCES AGAINST UNAUTHORIZED ACCESS, MODIFICATION, DESTRUCTION, OR DISCLOSURE**

The office should implement adequate controls to protect its information resources against unauthorized access, modification, destruction, or disclosure. This recommendation does not identify specific vulnerabilities that could allow someone to exploit the office's information system or misuse county funds. Disclosing those vulnerabilities could present a potential security risk by providing the readers with information that might be confidential pursuant to Section 10-7-504(i), Tennessee Code Annotated. We provided the official with detailed information regarding the specific vulnerabilities we identified, as well as our recommendations for improvement.

PRIOR AUDIT RECOMMENDATIONS IMPLEMENTED

(Ref: Review of Internal Controls Regarding Information System Operations as of January 2, 2003)

OFFICE OF CIRCUIT AND GENERAL SESSIONS COURTS CLERK

Finding Number	Page Number	Subject
-----------------------	--------------------	----------------

1	1	The Office Had Deficiencies in Computer System Back-up Procedures
---	---	---